IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,

CASE NO.: 1:23-CR-00056-JKB

vs.

BRANDON CLINT RUSSELL,

_____/

BRANDON RUSSELL'S MOTION TO COMPEL THE GOVERNMENT TO PROVIDE NOTICE OF ITS INTENT TO USE OR DISCLOSE INFORMATION OBTAINED OR DERIVED FROM SURVEILLANCE CONDUCTED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Brandon Russell files this Motion to Compel the government to provide him with notice of its intent to use or disclose information obtained or derived from surveillance under Section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a. Pursuant to 50 U.S.C. §§ 1806(c), 1806(e), and 1881e(a), as well as the Fourth and Fifth Amendments, Mr. Russell files this Motion and states the following in support:

Introduction

1. Brandon Russell is charged by Indictment with one count of conspiracy to damage an energy facility, which the government alleges constitutes an act of domestic terrorism. Indictment at 1-2 (ECF No. 25).

2. This Motion seeks to compel notice of the government's intent to use or disclose evidence obtained or derived from surveillance authorized by Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). Based on recent disclosures by the Federal Bureau of Investigation ("FBI") in the media and by FBI Director Christopher Wray, Mr. Russell has reason to believe that the government: (1) intercepted his communications pursuant to Section 702

without a warrant and (2) subjected him to what is often known as a "backdoor search"—a warrantless query of an American's communications within the government's Section 702 databases. The details provided to the media by a senior FBI official and then reiterated in a public speech by FBI Director Wray closely track the government's allegations in this case—from the nature of the alleged plot, to the means allegedly acquired to carry out the attack, to the alleged timeline of the events. Indeed, as explained below, the government appears to have subjected Mr. Russell to these warrantless searches to obtain information and evidence that the FBI claims was essential to the instant criminal investigation and prosecution. *See* John Sakellariadis, *FBI Reveals Controversial Spy Tool Foiled Terror Plot as Congress Debates Overhaul*, Politico (Feb. 13, 2024), https://www.politico.com/news/2024/02/13/fbi-surveillance-terrorist-attack-00141200# ("Politico Article") (Exhibit A); *Director Wray's Remarks to the ABA Standing Committee on Law and National Security*, FBI (Apr. 9, 2024), https://www.fbi.gov/news/speeches/director-wrays-remarks-at-the-aba-standing-committee-on-law-and-national-security ("Wray Speech") (Exhibit B).[1]

3. By statute, and as a matter of due process, Mr. Russell is entitled to notice of the government's intent to use evidence obtained or derived from Section 702 surveillance of his communications in the present case. *See* 50 U.S.C. §§ 1881e(a) & 1806(c); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 421 (2013); *United States v. Moalin*, 973 F.3d 977, 999–1001 (9th Cir. 2020). As described below, the government has a track-record of failing to provide the required notice in criminal prosecutions. But given the allegations in this case and the FBI's public disclosures, there is every reason to believe that Mr. Russell is entitled to notice of Section 702 surveillance here. Mr. Russell seeks such notice so that he may bring an informed motion to

[1] Defense counsel only recently learned of these FBI disclosures and their potential implications for this case. Accordingly, Mr. Russell respectfully requests leave to file this motion out of time.

suppress challenging the government's warrantless surveillance and querying of his communications. *See, e.g.*, *United States v. Hasbajrami*, 945 F.3d 641, 669–73 (2d Cir. 2019); 50 U.S.C. § 1806(e).

Section 702 Surveillance and the Notice Requirement

4. The government uses Section 702, 50 U.S.C. § 1881a, to intercept immense quantities of international communications, including many communications involving Americans. It does so by "targeting" hundreds of thousands of foreigners located abroad. *Id.* § 1881a(a); *see generally Report on the Surveillance Program Operated Pursuant to Section 702 of FISA*, Priv. & Civ. Lib. Oversight Bd. (Sept. 28, 2023) (hereinafter, "PCLOB Report").[2] Because many of those foreigners communicate with people in the United States, the government's surveillance routinely sweeps up Americans whose communications are entitled to constitutional protection. *See id.* The government stores the intercepted communications in intelligence agency databases, retains them for years, and searches them repeatedly for information about Americans—including in domestic criminal investigations. *Id.* This surveillance takes place inside the United States, with the compelled assistance of major communications providers and technology companies. *Id.*

5. All of this surveillance is conducted without a warrant or any individualized judicial approval. A crucial difference between Section 702 and traditional FISA is that Section 702 authorizes surveillance *without* probable cause or individualized suspicion. With respect to U.S. persons, Section 702 allows the government not just to warrantlessly collect, but to retain, query, review, and use U.S. persons' communications with targeted persons. No court reviews the government's targets or approves the government's subsequent use of this surveillance to

[2] *Available at* https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

investigate individual Americans. The Foreign Intelligence Surveillance Court ("FISC") has only limited involvement, conducting an annual review of the general procedures the government proposes to use in carrying out the surveillance program as a whole. *See* 50 U.S.C. § 1881a.

6. Because this surveillance often implicates the constitutionally protected privacy interests of people in the United States, Section 702 requires notice in certain circumstances. The statute provides:

> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

50 U.S.C. § 1806(c); *see* 50 U.S.C. § 1881e(a) (applying § 1806 to Section 702 surveillance).

7. The Supreme Court has recognized that notice of Section 702 surveillance in criminal cases is essential to ensuring judicial review of these warrantless searches. In *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the Supreme Court held that although the plaintiffs lacked standing, Section 702 was not insulated from judicial review in part because "if the Government intends to use or disclose information obtained or derived from a [Section 702] acquisition in judicial or administrative proceedings, it *must* provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition." *Clapper*, 568 U.S. at 421 (citing 50 U.S.C. §§ 1806(c),1806(e), 1881e(a)) (emphasis added). In doing so, the Supreme Court indicated that one important avenue for judicial review of the government's warrantless surveillance program is criminal or administrative proceedings where Section 702 information is at issue. *Id*. The government, for its part, agreed. *See* Gov. Br. at 8, *Clapper v. Amnesty Int'l USA*,

No. 11-1025, 568 U.S. 398 (2013), https://www.justice.gov/d9/osg/briefs/2012/01/01/2011-1025.mer.aa.pdf ("If the government intends to use or disclose any information obtained or derived from its acquisition of a person's communications under Section [702] in judicial or administrative proceedings against that person, it *must* provide advance notice of its intent to the tribunal and the person, whether or not the person was targeted for surveillance under Section [702]." (emphasis added)).

The FBI's Disclosures and the Surveillance of Mr. Russell

8. On February 13, 2024, Politico published an article—based on "newly declassified" information by the FBI—that strongly suggests that communications related to the instant prosecution were intercepted and queried pursuant to Section 702. Politico Article. According to the Article, "[t]he FBI revealed it used a controversial foreign surveillance tool to foil a terrorist plot on U.S. soil last year, part of a series of last-minute disclosures it hopes will sway Congress as lawmakers debate overhauling the measure later this week." *Id.* at 2. "The bureau shared three newly declassified instances with POLITICO in which its access to data collected under the digital spying authority—codified in Section 702 of the Foreign Intelligence Surveillance Act—allowed it to protect national security, **including one in which it thwarted a 'potentially imminent terrorist attack' against U.S. critical infrastructure last year**." *Id.* (emphasis added).

9. FBI Director Wray reiterated many of the same details in a public speech two months later. Wray Speech; *see also Warrant Requirement for FBI's Section 702 Queries Would Impede Investigations, Endanger National Security, Director Says*, FBI (Apr. 9, 2024), https://www.fbi.gov/news/stories/warrant-requirement-for-fbi-s-section-702-queries-would-impede-investigations-endanger-national-security-director-says (hereinafter "FBI News Story") (Exhibit C).

10. The February Politico Article and Director Wray's April speech contain details about the FBI's use of Section 702 surveillance to investigate an alleged attack on critical infrastructure. Together they indicate the FBI investigated Mr. Russell by querying its databases created under Section 702 to access his communications. Consider the following seven points:

11. First, the FBI investigation described in the Article involved an alleged "terrorist attack against U.S. critical infrastructure." Politico Article at 2. This prosecution undoubtedly involves critical infrastructure; Mr. Russell and his co-defendant Ms. Clendaniel are charged with conspiracy to damage an energy facility, in violation of 18 U.S.C. § 1366(a). Indictment at 1-2. Notably, the government has repeatedly referred to this prosecution as related to domestic "terrorism." *See, e.g.*, Press Release, *Maryland Woman and Florida Man Charged Federally for Conspiracy to Destroy Energy Facilities*, Dep't of Justice (Feb. 6, 2023), https://www.justice.gov/opa/pr/maryland-woman-and-florida-man-charged-federally-conspiring-destroy-energy-facilities (labeling the case as "domestic terrorism" and referring to "domestic violent extremists" and threats to "critical infrastructure").

12. Second, the senior FBI official stated that "a person located inside the U.S." had "already identified specific targets in the U.S." Politico Article at 3. The Affidavit in support of the Criminal Complaint and the Stipulation of Facts, included as part of Ms. Clendaniel's Plea Agreement, both allege that Ms. Clendaniel had identified five particular electrical substations in Maryland that she planned to target. *See* Affidavit in Support of Crim. Compl. (ECF No. 14-1 ¶¶ 14, 22–25) ("Affidavit"); Stip. of Facts, Clendaniel Plea Agreement (ECF No. 93 at 4–5) ("Stip. of Facts"). Further, Mr. Russell and Ms. Clendaniel were in the United States at the time of the alleged events in question.

13. Third, the Politico Article states that the "FBI revealed it used a controversial foreign surveillance tool to foil a terrorist plot on U.S. soil *last year*." Politico Article at 2 (emphasis added). Both Mr. Russell and Ms. Clendaniel were arrested "last year," on February 3, 2023, which presumably marks the "foiling" of the alleged attack. *See* Arrest Warrant (ECF No. 46) (Clendaniel); Arrest Warrant (ECF No. 1) (Case No. 23-mj-1120, M.D. Fla. Feb. 6, 2023) (Russell).

14. Fourth, the FBI told Politico that the alleged attack was "potentially imminent" and that the "FBI foiled the plot roughly 30 days after first uncovering it." Politico Article at 2, 3. Here, the government alleges the attack involved a "time frame" of "no longer than a month." *See* Affidavit ¶ 14; Stip. of Facts at 3. Although Ms. Clendaniel stipulated that the conspiracy began in December 2022, Stip. of Facts at 1, it appears the alleged "plot" was only "uncovered" by the FBI in January 2023—less than a month before Mr. Russell's and Ms. Clendaniel's arrests on February 3, 2023. The government alleges that Mr. Russell discussed the substation attack with a confidential human source on January 12, 2023, and that the source was first introduced to Ms. Clendaniel on that date. Affidavit ¶¶ 12–13; Stip. of Facts at 2. *See also* Press Release, *Maryland Woman Pleads Guilty to Conspiring to Destroy the Baltimore Region Power Grid*, Dep't of Justice (May 14, 2024), https://www.justice.gov/opa/pr/maryland-woman-pleads-guilty-conspiring-destroy-baltimore-region-power-grid (noting that the "plans began to culminate on Jan. 12, 2023"). This timeline falls within the "roughly 30 days" described in the Politico Article.

15. Fifth, based on the FBI's description, the Politico Article states that "a person located inside the U.S." had "acquired the means to conduct an attack." Politico Article at 3. The government alleges here that the purported attack involved shooting at electrical substations. Affidavit ¶ 14; Stip. of Facts at 3. The government further alleges that Ms. Clendaniel acquired

the firearms to carry out the alleged attack, and that agents recovered firearms and ammunition in Ms. Clendaniel's bedroom. *See* Affidavit ¶¶ 17–18; Stip. of Facts at 3–5.

16. Last, the FBI stated that "a person located inside the U.S. was in regular contact with an unspecified foreign terrorist group." Politico Article at 3. The government alleges that Mr. Russell was involved with the Atomwaffen Division, a National Socialist Group, which "reportedly has international ties" and has been listed as a "terrorist group" by a number of U.S. allies. Affidavit ¶¶ 4–5.[3] Additionally, based on information available to the defense, Mr. Russell appears to have been in frequent communication with individuals located abroad prior to his arrest.

17. FBI Director Wray confirmed many of the same details in a public speech in April. *See generally* Wray Speech. As the FBI's coverage of the speech recounts:

> For example, in 2023, the FBI was able to prevent a potential attack on U.S. critical infrastructure by a U.S. person who'd done relevant research and preparation and who'd been in touch with a foreign terrorist, Wray said. "Only by querying that U.S. person's identifiers in our 702 collection did we find important intelligence on the seriousness and urgency of the threat," he explained.
>
> Wray said the FBI was able to disrupt the would-be attacker less than a month after it conducted its first Section 702 query related to that subject. But, he noted, this query would've been impossible if a warrant requirement had been in place due to probable cause and exigency. "And if we hadn't done that query, we would've lost valuable time we needed to get ahead of the potential attack," he said.

FBI News Story at 3. As with the Politico Article, the government's allegations in this case match the facts laid out by FBI Director Wray as he described the FBI's use of warrantless Section 702 queries and urged Congress to reauthorize the warrantless surveillance program.

---

[3] *See, e.g.*, U.S. State Dep't, *Country Reports on Terrorism 2022: Australia*, https://www.state.gov/reports/country-reports-on-terrorism-2022/australia (last visited June 8, 2024) ("In February, Australia designated the National Socialist Order, formerly known as Atomwaffen Division, as a terrorist group."); Public Safety Canada, *Currently Listed Entities*, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx (last visited June 8, 2024); United Kingdom Home Office, *Proscribed Terrorist Groups or Organisations* (Apr. 26, 2024), https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2/proscribed-terrorist-groups-or-organisations-accessible-version.

18. Based on a search of federal criminal dockets and Department of Justice press releases since January 2023, this prosecution is the only case involving allegations that track the details in the Politico Article and FBI Director Wray's speech.

19. Given the details set forth above, it appears that at least some of the evidence that was obtained about Mr. Russell in the present case was acquired from surveillance of his communications under Section 702 of FISA.

Mr. Russell is Entitled to Notice

20. The government is required by statute and as a matter of due process to provide Mr. Russell with notice of its intent to use information "obtained or derived from" Section 702 surveillance of his communications in this prosecution. *See supra* ¶¶ 3, 6–7 (citing 50 U.S.C. §§ 1806(c), 1881e(a); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013); *United States v. Moalin*, 973 F.3d 977, 999–1001 (9th Cir. 2020)).

21. The FBI's disclosures in the Politico Article and FBI Director Wray's speech leave little doubt that the government relied on Section 702 surveillance to learn about the purported "terror attack" and develop its evidence in this case. The FBI claimed that Section 702 surveillance—which the Politico Article describes as a "controversial spy tool"—was what "foil[ed]" the "terrorist plot." Politico Article at 2; *see also id.* at 1 ("The bureau says it thwarted an imminent terrorist attack against the U.S. using a controversial surveillance authority . . . ."). The Article repeats similar FBI claims, at least three additional times. *First*, "the FBI official said the ability to search the Section 702 database without a court order *showed* that a person located inside the U.S. was in regular contact with an unspecified foreign terrorist group, had acquired the means to conduct an attack and had already identified specific targets in the U.S." *Id.* at 3 (emphasis added). *Second*, "[t]he FBI official argued the bureau almost definitely could not have

recreated its success" without Section 702. *Id.* at 4 (noting that a senior FBI official "said the [Section 702] searches were what revealed an attack was imminent in the first place." *Id.* at 5. *Third*, the Politico Article quotes the senior FBI official as stating "[i]f we hadn't done the query [of Section 702 databases], we would have lost valuable time we need to get ahead of a potential attack." *Id*. at 5. Importantly, FBI Director Wray confirmed the government's reliance on Section 702 surveillance and queries as well. He stated that "only by querying that U.S. person's identifiers in our 702 collection did we find important intelligence on the seriousness and urgency of the threat." Wray Speech at 9.

22. The government has a long track-record of failing to provide notice of Section 702 surveillance. For five years after Section 702's enactment, from 2008 to 2013, the government did not give notice to a single accused person. Only after several people in criminal cases moved to compel notice did the public learn that the Department of Justice had a practice of concealing the use of Section 702 in criminal cases. *See* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. Times (July 15, 2013), https://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html. The Department of Justice, it turned out, had adopted an unjustifiably narrow definition of a key term: when evidence is "derived from" Section 702 surveillance. *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times (Oct. 16, 2013), https://nyti.ms/2NmNFpS.

23. In response to the ensuing public scrutiny, the Department of Justice modified its notice policy behind closed doors and gave notice to eleven people between 2013 and 2018. *Id.*; Sarah Taitz & Patrick Toomey, *Concealing Surveillance: The Government's Disappearing Section 702 Notices*, Just Security (Sept. 27, 2023), https://www.justsecurity.org/88861/concealing-surveillance-the-governments-disappearing-section-702-notices/.

24. But over the past six years, those notices have inexplicably disappeared once again—no criminally accused has received notice of Section 702 surveillance since 2018. *See id.* That is despite the fact that FBI agents have searched through Section 702 databases for Americans' communications *millions* of times over the same period, and despite the government's claims that Section 702 surveillance provides invaluable access to Americans' communications for both intelligence and law enforcement investigations.[4] Moreover, the government's notice policy remains secret to this day, meaning it is impossible to assess how it is interpreting and applying key terms—like "derived from"—in FISA's notice provision.

25. Under the Fourth Amendment, the Fifth Amendment, and FISA, Mr. Russell is entitled to such notice. *See Berger v. New York*, 388 U.S. 41, 60 (1967) (finding wiretapping statute unconstitutional because, among other things, it had "no requirement for notice as do conventional warrants"); 50 U.S.C. §§ 1806(c), 1881e(a). Due process requires that the accused have a meaningful opportunity to suppress the fruits of illegally acquired evidence. *See, e.g.*, *Moalin*, 973 F.3d at 999–1001; *Jencks v. United States*, 353 U.S. 657, 671 (1957) (the government cannot invoke its privileges to "deprive the accused of anything which might be material to his defense"); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 318–24 (1972), (compelling disclosure of surveillance transcripts in a national security case); *Alderman v. United States*, 394 U.S. 165, 180–88 (1969) (same). As in other cases involving surreptitious surveillance, Mr. Russell seeks notice so that he may bring an informed motion to suppress challenging the government's warrantless surveillance and querying of his communications.

[4] *See Annual Statistical Transparency Report*, Off. of Dir. of Nat'l Intel., at 25, 35 (Apr. 2024), https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf; *Annual Statistical Transparency Report*, Off. of Dir. of Nat'l Intel., at 21 (Apr. 2022), https://www.intelligence.gov/assets/documents/702%20Documents/statistical-transparency-report/2022_IC_Annual_Statistical_Transparency_Report_cy2021.pdf; Wray Speech.

26. Additionally, to the extent the government warrantlessly surveilled and queried Mr. Russell's communications under Section 702 but claims that its evidence is not "derived from" this surveillance, that question must be litigated in an adversarial proceeding—not *ex parte*. *See Alderman*, 394 U.S. at 183–85 (in case involving the wiretapping of foreign spies, holding that the question of whether the government's evidence is "fruit of the poisonous tree" is so factually and legally complex that it cannot be litigated on an *ex parte* basis). The defense should have the opportunity to fully address any arguments raised by the government in response to this motion.

27. Finally, it is Black Letter Law that should the government's databases contain exculpatory and/or impeachment material, the Fifth Amendment requires the government to disclose such material.

Conclusion

28. For the foregoing reasons, Mr. Russell respectfully requests that this Court compel the government to provide the defense with notice of its intent to use or disclose information obtained or derived from Section 702 surveillance of his communications in the present case.

29. The defense contacted Assistant United States Attorney Kathleen Gavin. She stated that the government opposes the Motion.

30. Based upon the above-stated arguments, Mr. Russell maintains that the government has not provided the proper notice and therefore requests that the Court grant this Motion. Accordingly, the defense respectfully request that this Honorable Court enter its (attached and proposed) Order compelling the government to provide him with notice of its intent to use or disclose information obtained or derived pursuant to Section 702 of FISA.

Dated: June 11, 2024

Respectfully submitted,

/s/ Ian J. Goldstein

Ian J. Goldstein (Admitted *pro hac vice*)

LAW OFFICES OF IAN GOLDSTEIN P.A.
330 Clematis Street, Suite 209
West Palm Beach, FL 33401
Tel: (561) 600-0950

/s/ Kobie A. Flowers
Kobie A. Flowers (Bar No. 16511)

Brown, Goldstein & Levy, LLP
120 E. Baltimore Street, Suite 2500
Baltimore, Maryland 21202
Tel: (410) 962-1030

Counsel for Brandon Russell

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was electronically filed via CM/ECF which will serve all parties of record on this 11th day of June, 2024.

Respectfully submitted,

/s/ Ian J. Goldstein
Ian J. Goldstein (Admitted *pro hac vice*)

LAW OFFICES OF IAN GOLDSTEIN P.A.
330 Clematis Street, Suite 209
West Palm Beach, FL 33401
Tel: (561) 600-0950

Exhibit A

POLITICO

CYBERSECURITY

FBI reveals controversial spy tool foiled terror plot as Congress debates overhaul

The bureau says it thwarted an imminent terrorist attack against the U.S. using a controversial surveillance authority that the House could vote to revamp as soon as this week.

The bureau shared three newly declassified instances in which it said access to data collected under the digital spying authority allowed it to protect national security. | John Minchillo/AP

By JOHN SAKELLARIADIS
02/13/2024 02:41 PM EST

The FBI revealed it used a controversial foreign surveillance tool to foil a terrorist plot on U.S. soil last year, part of a series of last-minute disclosures it hopes will sway Congress as lawmakers debate overhauling the measure later this week.

The bureau shared three newly declassified instances with POLITICO in which its access to data collected under the digital spying authority — codified in Section 702 of the Foreign Intelligence Surveillance Act — allowed it to protect national security, including one in which it thwarted a "potentially imminent terrorist attack" against U.S. critical infrastructure last year.

The spying tool is set to expire in April if Congress does not renew it.

The House is expected to vote as early as Thursday on whether to approve a major change to the foreign surveillance authority, which has faced backlash because it also sweeps in data from Americans. That change would require bureau analysts to acquire a warrant or court order before searching a database of emails, texts and other digital communications of foreigners for information on U.S. citizens.

The proposal has support from lawmakers in both parties, and the FBI is on a campaign to sway those who are undecided or willing to reconsider.

"The big point here is the warrant requirement and how damaging that would potentially be, if it were adopted as part of a legislation," argued a senior bureau official speaking on behalf of the FBI, who was granted anonymity to freely discuss the cases in detail.

In the terrorist case, the FBI official said the ability to search the Section 702 database without a court order showed that a person located inside the U.S. was in regular contact with an unspecified foreign terrorist group, had acquired the means to conduct an attack and had already identified specific targets in the U.S.

The FBI foiled the plot roughly 30 days after first uncovering it, the official said.

Those searches were also key to unraveling a foreign adversary's efforts to illicitly acquire technology that can be used in biological weapons production. And in a third case, they revealed that the subject of one national security investigation was actively communicating with multiple foreign intelligence suspects tracked by other bureau field offices — a discovery the FBI feels could have been blown if it had resorted to slower, more overt investigative tools, like a warrant.

On Wednesday, the House Rules Committee will consider a compromise bill to update and renew Section 702. Lawmakers are then expected to vote on an amendment on the court order proviso if it gets sent to the House floor,

The lower chamber vote is critical since the White House has come out vigorously against the idea, and it will likely face stiffer opposition in the Democratic-led Senate.

A special federal court overseeing the program has uncovered a raft of compliance violations at the FBI since 2020, including instances in which bureau personnel improperly accessed the communications of Jan. 6 rioters, George Floyd protestors, and roughly 19,000 donors to an unnamed Congressional campaign.

Though assessments show internal FBI reforms in the last two years have significantly reduced those problems, a bipartisan cohort of lawmakers has argued that judicial guardrails are one of the only ways to prevent future violations of Americans' privacy.

The FBI and the Biden administration have repeatedly countered that those restrictions could cripple one of the country's most valuable intelligence tools.

National security adviser Jake Sullivan will deliver a classified briefing to House Democrats on the looming vote on Wednesday afternoon. In an email announcing the briefing that was obtained by POLITICO, Rep. Jim Himes (D-Conn), the ranking member of the House Intelligence Committee, warned that approving the amendment on the court order would "badly damage our national security."

In the examples shared by the FBI, the agency was unusually specific about the drawbacks of proposed reforms up for consideration in Congress.

The FBI official argued the bureau almost definitely could not have recreated its success in any of the three cases even if a court order mandate included an exception for national security matters — an idea that is popular among privacy advocates.

In the terrorism case, for example, the official said the searches were what revealed an attack was imminent in the first place.

"If we hadn't done the query, we would have lost valuable time we need to get ahead of a potential attack," the official argued.

FILED UNDER: CONGRESS, CYBER SECURITY, SURVEILLANCE, FBI, TERRORISTS,

Exhibit B

Christopher A. Wray
Director
Federal Bureau of Investigation

Washington, D.C.
April 9, 2024

Director Wray's Remarks to the ABA Standing Committee on Law and National Security

FBI Director Christopher Wray addresses the American Bar Association's Standing Committee on Law and National Security on April 9, 2024, in Washington, D.C.

Remarks as prepared for delivery

Thank you, Jason.

With the House taking up reauthorization of FISA [Foreign Intelligence Surveillance Act] Section 702 this week, it's timely that I'm in front of you today. This committee, the oldest Standing Committee in the ABA [American Bar Association], has for more than 60 years committed to educating the bar and the public on the importance of the rule of law in preserving both the freedoms of democracy and our national security. Principles that we at the FBI have always strived to adhere to. Principles that I believe set the American legal system, and our law enforcement and national security agencies, apart from our adversaries.

The Evolving Threat Landscape

That brings me to the first topic I'd like to discuss today: the evolving national security threat

landscape.

Today's national security threats are more complex and sophisticated than ever. We're seeing hostile nation-states becoming more aggressive in their efforts to steal our secrets and our innovation, target our critical infrastructure, and export their repression to our shores.

Front and center is China—the defining threat of our generation. To put it simply, the CCP [Communist Party of China] is throwing its whole government at undermining the security and economy of the rule-of-law world. China's hacking program is larger than that of every other major nation, combined. And if each one of the FBI's cyber agents and intelligence analysts focused exclusively on the China threat, China's hackers would still outnumber FBI cyber personnel by at least 50 to 1.

And it's not just cyber, but also traditional espionage and economic espionage, foreign malign influence, election interference, and transnational repression—often working in tandem. They recruit human sources to target our businesses, using insiders to steal the same kinds of innovation and data their hackers are targeting. They're engaging in corporate deception—hiding Beijing's hand in transactions, joint ventures, and investments—all with the same goal. They're exporting their repression efforts and human rights abuses—targeting, threatening, and harassing those who dare question their legitimacy or authority even outside China, including right here in the U.S.

We've seen professors and students on American campuses subjected to intense, almost Mafia-style pressure when they say things the CCP doesn't like, using their massive cyber operation to keep tabs on how dissidents in America are exercising their First Amendment rights online.

And of course, the PRC [People's Republic of China] plays the long game.

China's hackers have been positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities. China-sponsored hackers pre-positioned for potential cyberattacks against U.S. oil and natural gas companies way back in 2011.

Today, we're seeing China's increasing buildout of offensive weapons within our critical infrastructure. Setting up persistent PRC access in our critical sectors like telecommunications, energy, and water, poised to attack whenever Beijing decides the time is right.

Say when the PRC decides to invade Taiwan, and the Chinese government wants to cripple our military response. Because low blows aren't just a possibility in the event of a conflict. Low blows against civilians are part of China's plan.

Earlier this year, the FBI and our partners exposed China-sponsored hackers known as Volt Typhoon hiding inside our networks. The Volt Typhoon malware enabled China to hide, among other things, pre-operational reconnaissance and network exploitation against our critical infrastructure.

But working with our partners, the FBI ran a court-authorized, on-network operation to shut down Volt Typhoon and the access it enabled. That operation was an important step. But there's a lot more PRC cyber threat—in a lot more places—out there.

And of course, everyone here is well aware that China is not the only adversary we're up against. Russia and Iran are also determined to use every available tool at their disposal to take aim at things we all hold sacred—our freedoms, prosperity, and democratic norms.

Russia is a very sophisticated adversary, and they remain a top cyber threat. The Russian government continues to invest heavily in their cyber operations, in part because they see cyber as an asymmetric weapon to keep up with us. Like China, Russia continues to target critical infrastructure—including underwater cables and industrial control systems both in the United States and around the world.

Since its unprovoked invasion of Ukraine, we've seen Russia conducting reconnaissance on the U.S. energy sector. Adding to that concern is that the Russians—like our other adversaries—don't care if their cyber campaigns affect civilians. That's what we saw in 2017, when Russia's military used the NotPetya malware to hit Ukrainian critical infrastructure. They targeted Ukraine, but ended up also hitting systems throughout Europe, plus the U.S. and Australia. And even some systems within their own borders.

Showing the same wanton disregard for civilian safety through cyber that we're now seeing on display on the battlefield itself. They shut down a big chunk of global logistics, and ultimately, their recklessness ended up causing more than $10 billion in damages—maybe the most damaging cyberattack in history. And Russia continues its campaign to target our secrets, especially our military technology, in a variety of ways—from traditional spying to sophisticated cyber intrusions, signals collection platforms, and other technical means.

And then you've got Iran, which shouldn't be underestimated. They too are a very sophisticated, very aggressive cyber adversary and continue to engage in brazen behavior directed at us. In 2021, an Iranian-sponsored group conducted a cyber attack on a children's hospital in the United States. They're one of only two countries—the other being North Korea—to have conducted a destructive cyberattack inside the U.S. In recent years, individuals associated with Iran have plotted to assassinate a former U.S. National Security Advisor on American soil. And like China, they leverage covert means, including their cyber capabilities, to target dissidents and conduct transnational repression right here in the U.S.

An American journalist on U.S. soil has been targeted multiple times by Iranian intelligence officials, including most recently for assassination. Last year, we announced that the FBI and our partners had disrupted that assassination attempt, which Iran tried to carry out using an organized crime group. I have no doubt Iran will also continue to try to evade international sanctions by stealing our military technology through cyber hacking and illegal technology transfers—and of course, it remains the world's leading state sponsor of terrorism.

The Threat of Terrorism

And that brings me to the final threat I wanted to discuss today, and that's terrorism.

Terrorism is one of the most pressing national security challenges we face, and it remains the FBI's number one priority. I've been very public in saying that at a time when the terrorism threat was already elevated, the ongoing war in the Middle East has raised the threat of an attack against Americans inside the United States to a whole 'nother level.

One big reason for that is the steady drumbeat of calls for attacks we've seen from a veritable rogue's gallery of foreign terrorist organizations. Groups ranging from Hezbollah, to ISIS, to al-Qaida have publicly called for attacks against America and our allies. Hezbollah has publicly expressed its support and praise for Hamas and threatened to attack U.S. interests in the region. Al-Qaida issued its most specific call to attack the U.S. in the last 5 years. al-Qaida in the Arabian Peninsula—or AQAP—called on jihadists to attack Americans and Jewish people everywhere. And foreign terrorists, including ISIS, al-Qaida, and their adherents, have renewed calls for attacks against Jewish communities here in the United States and across the West in statements and propaganda.

As you probably know, these are groups that haven't always seen eye to eye—and that's

putting it mildly—now united in their calls for attacks on us. Given those calls for action, we cannot and do not discount the possibility that foreign terrorists may exploit the conflict to carry out an attack.

And while we continue to be concerned about individuals or small groups drawing twisted inspiration from the events in the Middle East to carry out attacks here at home. The foreign terrorist threat and the potential for a coordinated attack here in the homeland, like the ISIS-K [ISIS-Khorasan] attack we saw at the Russia Concert Hall a couple weeks ago is now increasingly concerning. October 7 and the conflict that's followed will feed a pipeline of radicalization and mobilization for years to come.

Summation of Threats

There's a lot of national security experience represented in this room. Many of you will remember when our government—our country—was almost exclusively focused on the fight against terrorism. In the 9/11-era against al-Qaida or ISIS at its height in, say, 2015 and 2016. And everyone here will be familiar with the Intelligence Community's more recent and much-discussed "pivot" to hard targets and great power competition.

What distinguishes the current moment is the breadth of national security threats we're facing all at once. None of the threats our country, our allies, are confronting is going away. In fact, the threats are only growing bigger.

On the nation state side, China, Russia, Iran—they're doubling down and heavily investing in their cyber, espionage, and foreign malign influence operations. And they're not remotely constrained by the rule of law.

They're tasking their criminals and "private sector" as strategic weapons against us—whether to hack our critical infrastructure, steal our military secrets, or gain an economic advantage against our businesses. All that at a time when the terrorist threat is very much still with us, and as I said earlier, has reached a whole 'nother level after October 7th.

America's adversaries aren't pulling any punches—they're coming at us with everything they've got. So, this is not the time for us to hang up our gloves or take away the tools that help us punch back.

FISA Section 702

That brings me to what the FBI is doing to stay ahead of and strategically disrupt these threats.

Our focus is not only whether we've got the resources—the money and the right talent to deal with these threats to grow to meet the challenges of the next five, 10 years. But also whether we've got the necessary tools to combat our adversaries.

And one tool that's indispensable to our efforts to combat threats posed by foreign adversaries, is one that will expire in just a couple of weeks if Congress does not act—and that's our FISA Section 702 authorities.

702 allows us to stay a step ahead of foreign actors located outside the United States who pose a threat to national security. And the expiration of our 702 authorities would be devastating to the FBI's ability to protect Americans from those foreign threats.

We're glad so many members of Congress support this critical tool, and our use of it, and recognize the value of 702 is undisputed. Whether it's to protect our critical infrastructure, find victims and get them the help they need, or detect foreign terrorists overseas directing an operative here to carry out an attack in our own backyard.

And crucial to our ability to use 702 to protect Americans is our ability to review intelligence promptly and efficiently through queries.

I've talked about how the PRC is pre-positioning on critical infrastructure across the United States. Just to pick an example: U.S.-person queries were key to discovering where Chinese hackers had successfully compromised network infrastructure at a transportation hub here in the United States, allowing us to alert the network operators so they could mitigate the intrusion.

Who knows how much damage those hackers could have caused—not just monetarily, but in the disruption and even the safety of Americans' lives. Effective and prompt victim notifications like those hinge on our ability to conduct U.S.-person queries of our existing 702 collection.

In just one recent cyber case, for instance, 702 allowed the FBI to alert more than 300 victims in every state and countries around the world—many of those notifications made possible because of U.S.-person queries. And U.S.-person queries, in particular, may provide the critical link that allows us to identify an intended target or build out the network

of attackers, so we can stop them before they strike.

And just like in cyber, U.S.-person queries continue to be key to identifying terrorists in the homeland, helping us find out who they're working with and what they're targeting—the intelligence we may need to stop them before they kill Americans. So, while it is imperative that we ensure this critical authority does not lapse, we also must not undercut the effectiveness of this essential tool with a warrant requirement or some similar restriction paralyzing our ability to tackle fast-moving threats.

Now, contrary to what a lot of folks are saying about the constitutionality and legality of U.S.-person queries, the law and the Fourth Amendment simply do not require a warrant in order for the FBI to query 702 data.

You don't have to take my word for it. Multiple federal district courts and appellate courts have considered the issue, and no court has ever held that a warrant is required for the FBI to conduct U.S.-person queries—to blind ourselves from information already lawfully in our holdings. And when the Foreign Intelligence Surveillance Court renews the 702 program every year, not once has it found that the law requires a warrant to conduct U.S.-person queries.

And if the appetite for a warrant is borne out of compliance concerns, I can wholeheartedly say that there are plenty of ways to ensure compliance without paralyzing us and our ability to move fast. We've proven that. I've been unequivocal that the compliance incidents we've had in the past are unacceptable. And in response, we've undertaken a whole host of reforms to ensure that we're good stewards of this authority.

Now, if you look at compliance reviews conducted by the Foreign Intelligence Surveillance Court and the Department of Justice on queries that were run after we put in place our reforms—let me say that again—the compliance reviews conducted on queries that were run after our reforms, both the FISC and DOJ have recognized that our reforms have resulted in substantial compliance improvements, hitting compliance rates well into the high 90% range.

And we're going to keep looking for ways to push that number even higher. So, if there's no constitutional, legal, or compliance necessity for a warrant requirement, then Congress would be making a policy choice to require us to blind ourselves to intelligence in our holdings. And if that's the path that's chosen, I can tell you that it will have real-world

consequences on our ability to disrupt the threats I outlined—on our ability to protect the American people.

Take for example a foreign terrorist organization—ISIS or al-Qaida—legally or illegally sending an operative into the U.S. to conduct an attack. U.S.-person queries on the foreign terrorist's communications are how we're able to potentially learn the extent of what they're planning and how imminent it may be.

Requiring a warrant for U.S.-person queries—which are typically conducted in the nascency of an investigation; when we usually cannot establish probable cause or demonstrate exigency; where time is of the essence to get ahead of the bad guys—would be a deliberate and shortsighted choice to blind us to the threat of a foreign terrorist in the U.S. planning and even executing an attack.

The consequences of tying our hands are not merely hypothetical. Just last year, we discovered that a foreign terrorist had communicated with a person we believed to be in the United States. Only by querying that U.S. person's identifiers in our 702 collection did we find important intelligence on the seriousness and urgency of the threat. And less than a month after that initial query, we disrupted that U.S. person who, it turned out, had researched and identified critical infrastructure sites in the U.S. and had acquired the means to conduct an attack.

If we had to obtain a warrant to conduct that initial query, based on what we knew at that time, there is no way we could've met a probable cause standard or even an exigency exception. And if we hadn't done that query, we would've lost valuable time we needed to get ahead of the potential attack.

Bottom line, a warrant requirement would be the equivalent of rebuilding the pre-9/11 intelligence "wall." I saw the consequences of that policy choice 22 years ago. I've spoken with families of victims of that horrific attack. And now two decades later, I can assure you that none of our adversaries are holding back or tying their own hands—whether to attack us, steal from us, to put American national security, our economic security, and American lives at risk.

So we need lawyers—folks like you who are committed to educating the bar and the public on the rule of law and our national security to explain what's law and what's policy, what a warrant is and what it isn't, and to help illuminate the consequences of purposefully

choosing to limit the American Intelligence Community from accessing key and timely information about our foreign adversaries.

Because we're in crunch time when it comes to reauthorizing this vital authority. And as the threats to our homeland continue to evolve, the agility and effectiveness of 702 will be essential to the FBI's ability—and really our mandate from the American people—to keep them safe for years to come.

And we owe it to them to make sure we've got the tools we need to do that.

Thank you for having me, and I look forward to your questions.

Resources:

- Story: Warrant Requirement for FBI's Section 702 Queries Would Impede Investigations, Endanger National Security, Director Says
- Inside the FBI Podcast: Making Sense of FISA Section 702
- Resource Page: Foreign Intelligence Surveillance Act (FISA) and Section 702

Exhibit C

April 9, 2024

Twitter Facebook Email

Warrant Requirement for FBI's Section 702 Queries Would Impede Investigations, Endanger National Security, Director Says

Wray says requirement would hinder our ability to combat cyberattacks, terrorism

FBI Director Christopher Wray addresses the American Bar Association's Standing Committee on Law and National Security on April 9, 2024, in Washington, D.C.

The FBI’s surveillance authorities under Section 702 of the Foreign Intelligence Surveillance Act are indispensable to the Bureau’s efforts to combat threats from foreign adversaries, Director Christopher Wray said on April 9.

But, he said, requiring the Bureau to obtain a warrant to query its database of information collected under its Section 702 authorities would hinder the FBI's ability to obtain and act upon threat intelligence and—by extension—to prevent potential terrorist or cyber-facilitated attacks against the homeland.

“If there’s no constitutional, legal, or compliance necessity for a warrant requirement, then Congress would be making a policy choice to require us to blind ourselves to intelligence in our holdings,” Wray told the American Bar Association’s Standing Committee on Law and National Security in Washington, D.C. Implementing such a requirement would have “real-world consequences” on the Bureau’s ability to disrupt terrorist and cybersecurity threats and “protect the American people,” he added.

Such a requirement would also impede our ability to quickly reach victims of cyber incidents, since U.S.-persons queries help power those timely notifications.

The Importance of U.S.-Persons Queries

According to Wray, U.S.-persons queries are usually conducted in the early stages of an investigation—when it's usually still too early to "establish probable cause or demonstrate" urgency.

These queries can help the FBI connect the dots between bad actors and their intended targets—or between bad actors and their criminal networks—so the Bureau can prevent attacks before they happen.

And since every second counts when you're racing to outpace a threat, any potential delay in obtaining threat intelligence could potentially cost lives.

For example, in 2023, the FBI was able to prevent a potential attack on U.S. critical infrastructure by a U.S. person who'd done relevant research and preparation and who'd been in touch with a foreign terrorist, Wray said. "Only by querying that U.S. person's identifiers in our 702 collection did we find important intelligence on the seriousness and urgency of the threat," he explained.

Wray said the FBI was able to disrupt the would-be attacker less than a month after it conducted its first Section 702 query related to that subject. But, he noted, this query would've been impossible if a warrant requirement had been in place due to probable cause and exigency. "And if we hadn't done that query, we would've lost valuable time we needed to get ahead of the potential attack," he said.

The Bureau's ability to run U.S.-persons queries also allowed us to gain awareness that Chinese hackers had compromised a U.S. transportation hub's network and flag the intrusion to hub personnel so they could respond, Wray said.

"Who knows how much damage those hackers could have caused—not just monetarily, but in the disruption and even the safety of Americans' lives," Wray said. "Effective and prompt victim notifications like those hinge on our ability to conduct U.S.-person queries of our existing 702 collection."

Addressing Legal and Compliance Questions

Neither the Fourth Amendment, nor the law, require the FBI to obtain a warrant before it can run a search against data collected under our Section 702 authorities, Wray added.

"Multiple federal district courts and appellate courts have considered the issue, and no court has ever held that a warrant is required for the FBI to conduct U.S.-person queries—to blind ourselves from information already lawfully in our holdings," he said. "And when the Foreign Intelligence Surveillance Court renews the 702 program every year, not once has it found that the law requires a warrant to conduct U.S.-person queries."

He also stressed that a warrant requirement isn't necessary to ensure that the FBI follows the law when it runs Section 702 queries. "We've proven that," he said. "I've been unequivocal that the compliance incidents we've had in the past are unacceptable. And in response, we've undertaken a whole host of reforms to ensure that we're good stewards of this authority."

Both the U.S. Department of Justice and the Foreign Intelligence Surveillance Court "have recognized that our reforms have resulted in substantial compliance improvements, hitting compliance rates well into the high 90% range," he noted, adding that the FBI will continue to brainstorm ways to further improve those rates.

Finally, he noted said that lawyers are critical to helping the general public make sense of law, policy, and the definition of a warrant, "and to help illuminate the consequences of purposefully choosing to limit the American Intelligence Community from accessing key and timely information about our foreign adversaries."

Resources:

- Resource Page: Foreign Intelligence Surveillance Act (FISA) and Section 702
- Inside the FBI Podcast: Making Sense of FISA Section 702

> **"If there's no constitutional, legal, or compliance necessity for a warrant requirement, then Congress would be making a policy choice to require us to blind ourselves to intelligence in our holdings."**

FBI Director Christopher Wray

Director Wray's Remarks to the ABA Standing Committee on Law and National Security

FBI Director Christopher Wray's remarks before the American Bar Association's Standing Committee on Law and National Security in Washington, D.C. on April 9, 2024

Inside the FBI Podcast: Making Sense of FISA Section 702

On this episode of Inside the FBI, Deputy Director Paul Abbate explains Section 702 of the Foreign Intelligence Surveillance Act: what it is, what it's not, and why you’ll likely be hearing a lot about it in the near future.